REMARKS

I. Introduction

Claims 1-21 are pending in the present application. In a November 1, 2006, Office Action (hereinafter "Office Action"), Claim 19 was rejected under 35 U.S.C. § 102(b) as being anticipated by a publication entitled "Internet Explorer Security Options, Part 2" to Smith (hereinafter "Smith"). Claims 1-3 and 10-12 were rejected under 35 U.S.C. § 103(a) as being obvious over a publication entitled "Description and Availability of Internet Explorer Error Reporting Tool" (hereinafter "KB276550") in view of a publication entitled "Document Viewer Installation and Getting Started" (hereinafter "WORD"). Claims 4 and 13 were rejected under 35 U.S.C. § 103(a) as being obvious over the KB276550 reference in view of WORD and in further view of Smith. Claims 5 and 14 were rejected under 35 U.S.C. § 103(a) as being obvious over the KB276550 reference in view of WORD, and in further view of a publication entitled "Microsoft Error Reporting" (hereinafter "MEP"). Claims 6, 7, 15, and 16 were rejected under 35 U.S.C. § 103(a) as being obvious over the KB276550 reference in view of WORD, and in further view of U.S. Patent No. 6,629,267 issued to Glerum et al. (hereinafter "Glerum"). Claims 8, 9, 17, and 18 are rejected under 35 U.S.C. § 103(a) as being obvious over the KB276550 reference in view of WORD, Glerum, and in further view of a publication entitled "Microsoft Computer Dictionary" (hereinafter "REG").

For the following reasons, applicants respectfully submit that the rejected claims of the present application are not anticipated and are non-obvious over the cited references because the cited references, alone or in combination, fail to teach or suggest generating a failure signature that is characteristic of a plug-in module. Prior to discussing more detailed reasons for applicants' belief that all the claims of the present invention are allowable, a brief description of the present invention and the cited references is presented. The following discussions of the

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206 682 8100

disclosed embodiments of applicants' invention and the teachings of the references are not provided to define the scope or interpretation of any of applicants' claims. Instead, such differences are provided to help the U.S. Patent and Trademark Office better appreciate important claim distinctions discussed thereafter.

A. Summary of the Present Invention

The present invention is generally directed to improving the stability of a Web browser by identifying plug-in modules that cause failures and permitting users to disable or update problematic plug-in modules. In one aspect, a method is provided for identifying a plug-in module that generated a failure. In response to receiving notice of a failure, the method obtains selected contents of memory from a computer created at the time of the failure. A failure signature is generated from the contents of memory that is characteristic of the plug-in module that generated the failure. Then, the newly created failure signature is compared with one or more failure signatures generated to identify the source of the failure.

B. Summary of KB276550

The KB276550 reference is directed to a Web browser error reporting tool that reports unrecoverable errors to a trusted entity over the Internet for analysis by developers. In this regard, KB276550 teaches a system in which users may view details about problems encountered while the Web browser executes and submits error information to a trusted entity. The information reported to the trusted entity allows developers to identify the source of the error. Based on the information that is received from a plurality of users, developers may create patches that are distributed in service packs at a later point in time. However, the KB276550 reference does not perform processing in real time that identifies a specific plug-in module that is the source of the error.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206 682 8100

C. Summary of the WORD Reference

The WORD reference is directed to a plug-in module that allows a user to view documents that are not in a format which may be natively viewed from a Web browser. More specifically, the WORD reference allows users to open and view Microsoft Word® documents while the user is employing a Web browser to locate and download information from a remote location. Instead of a user being required to open a separate program (e.g., Microsoft Word®) when a word processing document is downloaded, the user may view the document inside a Web browser program such as Microsoft Internet Explorer®. In this regard, the WORD reference discloses a system for installing a plug-in to a Web browser that allows users to view word processing documents identified while the user is browsing a computer network.

D. Summary of Smith

The Smith referenced is purportedly directed to configuring security settings for security zones in Microsoft Internet Explorer. In this regard, Smith discloses a way for users to define security policies while browsing a computer network. For example, from a graphical user interface, users may implement a security policy in which broad categories of plug-in modules are either automatically disabled or enabled. Also, in the Smith system a user may define a security policy in which a prompt is displayed in figure to obtain user feedback before a plug-in module to a Web browser program is allowed to execute.

II. The Claims Distinguished

A. Rejection Under 35 U.S.C. § 112

Claims 6, 8, 9, 15, 17, and 18 were rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter that applicants regard as the invention. These claims have been amended to overcome this rejection.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

B. Rejection Under 35 U.S.C. § 102

The Office Action rejected Claim 19 under 35 U.S.C. § 102 as being anticipated by Smith. As amended, Claim 19 recites the following:

> 19. A computer-readable medium bearing computer-executable instructions which, when executed:
>
> identifies plug-in modules used in conjunction with a Web browser;
>
> identifies a plug-in module that generated a failure;
>
> displays a graphical user interface that lists the plug-in modules used in conjunction with a Web browser; and
>
> supports disabling one or more of the plug-in modules used in conjunction with the Web browser.

Claim 19 is directed to a computer-readable medium that identifies and displays information about plug-in modules associated with a Web browser program. In this regard, when a Web browser program is executing and a failure occurs, the claimed subject matter identifies a plug-in module to the Web browser program that generated the failure. More specifically, the subject mater recited in Claim 19 "identifies a plug-in module that generated a failure." Moreover, from a user interface provided by aspects of the present invention, a user may disable the plug-in module that is identified as being the source of the failure. More specifically, as recited in Claim 19, the user interface "supports disabling one or more of the plug-in modules used in conjunction with the Web browser."

Simply stated, the Smith reference does not teach performing processing to identify a plug-in module that generated a failure. Instead, the Smith reference allows users to define security policies while browsing a network. Even though the Smith reference allows users to prevent entire categories of plug-ins to be installed, it does not teach identifying a specific plug-in module that generated a failure. For example, the teachings of Smith may allow a user to

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206 682 8100

prevent ActiveX controls from being installed. However, if an error condition occurred, the user would not be able to obtain information about the identity of the specific plug-in module that caused the error.

The Office Action asserts that the Smith reference supports disabling one or more of the plug-in modules to a Web browser. In support of that proposition, the Office Action cites FIGURE 2 of the Smith reference that depicts the use of radio buttons to enable/disable particular categories of plug-ins to a Web browser program. However, the referenced subject matter describes a system in which a user may implement a generalized security policy. In this regard, the user interface illustrated in FIGURE 2 of the Smith reference allows a user to implement a security policy in which the user may be prompted before a category of plug-in modules control is allowed to execute. Similarly, a user may implement a security policy that automatically disables or enables all plug-in modules for the selected category. Applicants respectfully submit that allowing a user to implement a security policy with regard to broad categories of plug-ins is not equivalent to allowing a user to disable one or more specific plug-in modules. More specifically, the Smith reference does not teach a system that "supports disabling one or more of the plug-in modules used in conjunction with the Web browser" as recited in Claim 19. Instead, the cited portion of Smith allows a user to implement a broad security policy with regard to categories of plug-in modules to a Web browser program. In this regard, Smith would not allow a user to disable/enable a specific plug-in module such as a Microsoft Word® viewer. Instead, Smith would only allow a user to enable/disable broad categories of plug-ins to a Web browser program (e.g., ActiveX controls, COM modules, and the like). Accordingly, Smith does not teach each of the elements recited in Claim 19.

Under Section 102(e), a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. *Verdegaal*

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206 682 8100

Bros. v. Union Oil Co. of California, 814 F.2d 628, 631 (Fed. Cir. 1987) (February 2003). Applicants respectfully submit that Smith fails to expressly or inherently teach, disclose, or suggest each and every element of Claim 19. As explained above, Smith fails to disclose or suggest identifying a plug-in module that generated a failure and allowing a user to disable a specific plug-in module that was identified as the source of the failure. Accordingly, applicants respectfully request withdrawal of the pending rejection under 35 U.S.C. § 102 with regard to Claim 19.

C. Rejections Under 35 U.S.C. § 103

1. Claims 1 and 10

For the purpose of this discussion, independent Claims 1 and 10 will be discussed together because the elements that distinguish each of these claims from the cited references are similar.

Claim 1 recites the following:

> 1. In a computing device having at least one plug-in module that extends the functionality of a Web browser, a method of identifying a plug-in module that generated a failure, comprising:
>
> in response to receiving notice of a failure, obtaining selected contents of memory of said computing device created at the time of the failure;
>
> generating a failure signature that is characteristic of the plug-in module that generated the failure; and
>
> comparing said failure signature with one or more failure signatures generated by known plug-in modules.

Similarly, Claim 10 recites the following:

> 10. A computer-readable medium bearing computer-executable instructions that, when executed, carry out a method of identifying a plug-in module that generated a failure, comprising:

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206 682 8100

in response to receiving notice of a failure, obtaining selected contents of memory of said computing device created at the time of the failure;

generating a failure signature that is characteristic of the plug-in module that generated the failure; and

comparing said failure signature with one or more failure signatures generated by known plug-in modules.

Claims 1 and 10 are directed to performing processing to identify a plug-in module to a Web browser that caused a failure. In this regard, each of these claims recites processes and steps for generating a failure signature and comparing the failure signature to signatures associated with known plug-in modules. By performing these steps, aspects of the present invention allow a user to identify a specific plug-in module that is the source of a failure. Some existing systems allow a user to report errors to a trusted entity. However, these existing systems do not allow a user to obtain information about a specific plug-in module that is the source of the failure.

The KB276550 reference does not teach "generating a failure signature that is characteristic of the plug-in module that generated the failure" and "comparing said failure signature with one or more failure signatures generated by known plug-in modules," as recited in Claims 1 and 10. The Office Action asserts that the KB276550 reference teaches generating a failure signature that is characteristic of the module that generated the failure and cites pages 3-4 of the KB276550 reference in support of that proposition. This cited portion of the KB276550 reference describes a system in which an error reporting tool directs the user to a location where a "patch" or "workaround" may be obtained. More specifically, the cited portion of the KB276550 reference states that, "[i]f a patch or workaround exists for the specific issue you reported, the Internet Explorer Error Reporting tool directs you to the appropriate Web site where you can download the patch or workaround. . . ." KB276550 at page 4. In this regard, the

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206 682 8100

Office Action asserts that the step of comparing a failure signature characteristic of a plug-in module is implied in the cited portion of the KB276550 reference. Office Action at page 5. In making this proposition, the Office Action assumes that a failure signature is generated in the KB276550 system to identify the appropriate patch to apply. However, this assertion in the Office Action reads teaching into the KB276550 that are not accurate. Those skilled in the art and others will recognize that systems that identify patches for a computer do not generate failure signatures. Instead, in order to identify an appropriate patch, the software state of a computing device is analyzed. In this regard, the version of an operating system, application programs, and all of the previously installed software updates are identified. Then, a database maintained by developers is queried for information about available software updates given the software state of the computer. In other words, to identify which patch should be installed, the software state of the computing device is identified and a lookup is performed to determine which patches are appropriate given the computer's software state. For example, rules maintained by developers may dictate that, given the operating system installed on a computer (e.g., Microsoft Windows 98®) and the version of the Web browser (e.g., Internet Explorer® 5.02), one or more applicable patches should be installed. Applicants respectfully submit that performing a lookup to identify the software state of a computer and determining which patches are appropriate is not equivalent to generating a failure signature to identify a specific plug-in module that is the source of a failure.

In contrast to the KB276550 reference, aspects of the present invention generate a failure signature that is characteristic of a specific plug-in module that generated the failure. In this regard, failure signatures are maintained in a database that is referenced when a failure occurs. As stated in the present application, each record in the database contains a signature that is unique to each plug-in module. More specifically, the present application states:

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206 682 8100

> In each record, the APPLICATION NAME 402 and APPLICATION VERSION 404 fields store the application name and version that was executing at the time of the failure. The LIBRARY NAME 406 and LIBRARY VERSION 408 fields store the name and version number that collectively identify the LIBRARY that generated the failure. The LIBRARY OFFSET 410 field stores a numeric value representative of the code location in the library where the failure occurred. The EXCEPTION CODE 412 field stores exception code generated by the operating system in response to the failure. As known to those skilled in the art, when a failure occurs, an operating system generates exception code that identifies the specific type of failure that occurred. The information contained in each record including database fields 402, 404, 406, 408, 410, and 412 collectively form a failure signature that is used by the present invention to identify plug-in modules that cause failures.

Present application at page 11. Since developers each build libraries designed to implement their individual plug-in modules, the set of libraries that is recorded in each record of the database is unique. Thus, the failure signature generated by aspects of the present invention uniquely identifies plug-in modules. In contrast, the KB276550 reference may not uniquely identify a plug-in module by generating a failure signature.

Aspects of the present invention may be implemented in conjunction with the system disclosed in the KB276550 reference. As mentioned previously, the KB276550 reference describes a system for reporting a failure that occurred in an application program. For example, if an error occurs, the KB276550 system may report information to a trusted entity. As an improvement to the system taught by the KB276550 reference, aspects of the present invention perform processing to generate a unique failure signature that is characteristic of a plug-in module to identify which plug-in module generated a failure. As a result, the user may choose to disable the specific plug-in module that was identified as the source of the failure. This is especially beneficial in instances when a software update does not exist to remedy the failure or the plug-in module that generated the failure is malware.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206 682 8100

In contrast to the elements recited in Claims 1 and 10, the KB276550 reference does not teach generating a failure signature that is characteristic of the plug-in module that generated the failure and comparing said failure signature with one or more failure signatures generated by known plug-in modules. Instead, as reflected in the cited portion of the KB276550 reference above, an appropriate patch may be identified from the software state of the computer. However, in instances when a patch is not available or the plug-in module is malware, users are not able to disable the plug-in module. Instead of a unique signature being generated, a lookup to identify the software state of the computer is performed and a database is referenced to identify an appropriate patch given the software state of the computing device.

Generally described, under 35 U.S.C. § 103(a), a *prima facie* case of obviousness can be established only if the cited references, alone or in combination, teach each and every element recited in the claim. (*In re Bell*, 991 F.2d 781 (Fed. Cir. 1993). However, neither the KB276550 or WORD references, alone or in combination, can be properly asserted as disclosing a method that includes generating a figure signature that is characteristic of a plug-in module. Thus, for the above reasons, applicants respectfully request withdrawal of the 35 U.S.C. § 103(a) rejections of Claims 1and 10.

2. Claims 2-3 and 11-12

Claims 2-3 and 11-12 depend on independent Claims 1 and 10, respectively. As discussed above, the KB276550 reference fails to teach or suggest generating a failure signature that is characteristic of the plug-in module and comparing said failure signature with one or more failure signatures generated by known plug-in modules. Accordingly, for the above-mentioned reasons, Claims 2-3 and 11-12 are also allowable over the applied references.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206 682 8100

3. Claims 4 and 13

Claims 4 and 13 were rejected under 35 U.S.C. § 103(a) as being obvious over the KB276550 reference, in view of WORD, and in further view of Smith. As discussed above, the KB276550 reference fails to teach or suggest generating a failure signature that is characteristic of the plug-in module and comparing said failure signature with one or more failure signatures generated by known plug-in modules. Accordingly, for the above-mentioned reasons, Claims 4 and 13 are also allowable over the KB276550 reference in view of the WORD reference, and in further view of Smith. Additionally, these claims are nonobvious for additional reasons, as discussed in further detail below.

Claims 4 and 13 include the additional element of "allowing the user to disable the plug-in module that generated the failure." The Office Action acknowledges that the KB276550 and WORD references fail to teach disabling a plug-in module that extends the functionality of a Web browser. However, the Office Action asserts that Smith teaches disabling a plug-in module that extends the functionality of a Web browser and references FIGURE 2 of Smith in support of that proposition. However, as described above, Smith allows users to implement a security policy for categories of plug-in modules. In this regard, a user is not able to identify and disable a specific plug-in module that was identified as the source of a failure. Accordingly, these claims are non-obvious over the cited references for this additional reason.

4. Claims 5-7 and 14-16

Claims 5-7 and 14-16 depend on independent Claims 1 and 10, respectively. As discussed above, the KB276550 reference fails to teach or suggest generating a failure signature that is characteristic of the plug-in module that generated the failure, among other claim elements. Accordingly, for the above-mentioned reasons, Claims 5-7 and 14-16 are allowable over the KB276550 reference in view of the various combinations of the WORD reference, MEP

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206 682 8100

reference, and Glerum. Additionally, these claims are nonobvious over the cited and applied references for additional reasons, some of which are discussed in further detail below.

Claims 6 and 15 include the additional elements of identifying a library that was executing at the time of the failure, determining the plug-in module that uses the library, and identifying the application that interacts with the plug-in module that uses the library. The Office Action asserts that the KB276550 reference teaches identifying an application that interacts with the plug-in module that uses a library and references page 3 of the KB276550 reference in support of that proposition. Applicants are unable to find any description of processing to identify a plug-in module that is associated with a particular library in the KB276550 reference. The cited portion of the KB276550 reference describes a way to disable an error reporting tool. Processing to identify a library where an error occurred is not disclosed. By contrast, aspects of the present invention perform processing to analyze a minidump file in order to identify a library that is associated with a plug-in module. See present application at page 9, lines 6-24. Accordingly, the KB276550 reference fails to teach or suggest the additional elements recited in Claims 6 and 15 as asserted in the Office Action and these claims are allowable for this additional reason.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206 682 8100

CONCLUSION

Based on the above-referenced arguments, applicants respectfully submit that all pending claims of the present application are patentable over the cited references. Because the cited references fail to teach or suggest each element of the pending claims, applicants respectfully request withdrawal of the rejections and allowance of the present application. If any questions remain, applicants request that the Examiner contact the undersigned at the telephone number listed below.

Respectfully submitted,

CHRISTENSEN O'CONNOR
JOHNSON KINDNESS^{PLLC}

Clint J. Feekes
Registration No. 51,670
Direct Dial No. 206.695.1633

CJF:jlg

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{PLLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206 682 8100